2/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI

012130152 **Image available**
WPI Acc No: 1998-547064/ 199847
XRPX Acc No: N98-426294

Network security system used during accounts settlement - starts service after comparing transmitted data with identification coding file, by server

Patent Assignee: OKI ELECTRIC IND CO LTD (OKID)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 10240691	A	19980911	JP 9759861	A	19970226	199847	B

Priority Applications (No Type Date): JP 9759861 A 19970226
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 10240691	A		13	G06F-015/00	

Abstract (Basic): JP 10240691 A

The system consists of a data acquisition unit (4) provided at client side, that acquires the characteristic data corresponding to the eyes of the user. A card input unit reads the identification code recorded in the card, when user inserts the card. The read characteristic data is compared with the acquired data.

If both data are equal, the specific user is confirmed. Then, the confirmed data is transmitted to sever, that comprises ID coding file. The server refers to the received data with the coding file, and starts service.

ADVANTAGE - Prevents individual information leakage and hence enhances security. Eliminates inaccurate process.

Dwg.1/12

Title Terms: NETWORK; SECURE; SYSTEM; ACCOUNT; SETTLE; START; SERVICE; AFTER; COMPARE; TRANSMIT; DATA; IDENTIFY; CODE; FILE; SERVE
Derwent Class: P31; T01
International Patent Class (Main): G06F-015/00
International Patent Class (Additional): A61B-003/10; A61B-005/117; G06F-017/60; G06T-007/00
File Segment: EPI; EngPI

2/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

05957591 **Image available**
NETWORK SECURITY SYSTEM

PUB. NO.: 10-240691 A]
PUBLISHED: September 11, 1998 (19980911)
INVENTOR(s): HOSHINO TADAHIRO
APPLICANT(s): OKI ELECTRIC IND CO LTD [000029] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 09-059861 [JP 9759861]
FILED: February 26, 1997 (19970226)
INTL CLASS: [6] G06F-015/00; A61B-003/10; A61B-005/117; G06F-017/60; G06T-007/00
JAPIO CLASS: 45.4 (INFORMATION PROCESSING -- Computer Applications); 28.2 (SANITATION -- Medical); 45.9 (INFORMATION PROCESSING -- Other)
JAPIO KEYWORD: R087 (PRECISION MACHINES -- Automatic Banking); R303

ABSTRACT

PROBLEM TO BE SOLVED: To secure safety by preventing feature data and an identification number, etc., from flowing through a network, eliminating the danger of the leakage of individual information and making no one other than the person himself/herself capable of gaining access to the service.

SOLUTION: A feature data obtaining part 4 obtains the feature data from the video images of the eyes of a user 9. In a card 5, the registered feature data of the user himself/herself are stored beforehand. When it is confirmed that the user 9 is a card owner himself/herself in a collation part 7, an identification code stored in the card 5 is sent from a client 1 to a server 3. The server 3 provides the client 1 with the service based on the identification code.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－240691

(43)公開日　平成10年(1998)９月11日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ
			３３０Ｇ
Ａ６１Ｂ　3/10		Ａ６１Ｂ　3/10	Ｚ
5/117		5/10	３２０Ａ
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	３４０Ｂ

審査請求　未請求　請求項の数７　ＦＤ　(全 13 頁)　最終頁に続く

(21)出願番号　特願平9－59861

(22)出願日　平成９年(1997)２月26日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　星野　恭祐
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

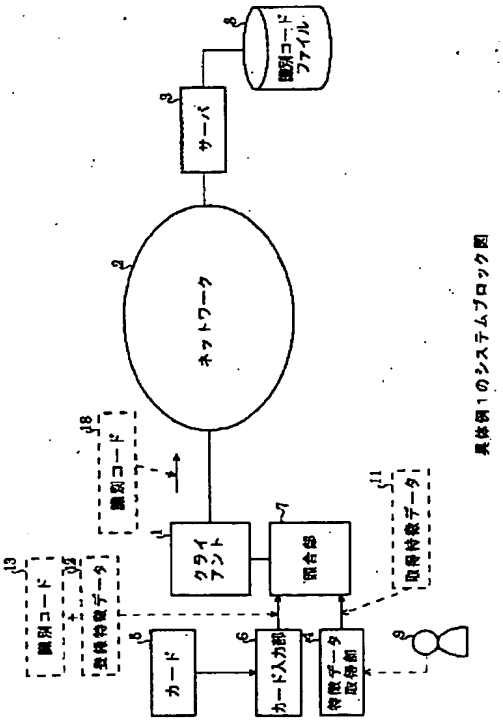
(74)代理人　弁理士　佐藤　幸男　(外１名)

(54)【発明の名称】　ネットワークセキュリティシステム

(57)【要約】

【解決手段】　特徴データ取得部４は、ユーザー９の眼の映像から特徴データを取得する。カード５には、予めユーザー本人の登録特徴データが格納されている。照合部７でユーザー９がカード所有者本人と確認されると、カード５に格納された識別コードがクライアント１からサーバ３に送られる。サーバ３は、この識別コードに基づいてクライアント１にサービスを提供する。

【効果】　ネットワーク２を特徴データや暗証番号等が流れないため個人情報の漏洩のおそれがなく、本人以外がサービスにアクセスできないため安全を確保できる。



具体例１のシステムブロック図

1

【特許請求の範囲】

【請求項１】　クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、

クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録された登録特徴データと、ユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取った登録特徴データと特徴データ取得部が取得したユーザーの眼の映像の特徴データとを照合して、ユーザーがカード所有者本人かどうかの確認を行う照合部を備え、

サーバ側には、正規のユーザーの識別コードを格納した識別コードファイルを備え、

クライアント側で前記照合処理の結果、ユーザーがカード所有者本人と確認したとき、クライアントからサーバに識別コードが送信され、

サーバは、識別コードファイルを参照して、ユーザーへのサービスを開始することを特徴とするネットワークセキュリティシステム。

【請求項２】　クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、

クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録されたファイル検索キーと、ユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取ったファイル検索キーにより登録特徴データファイルからカード所有者の登録特徴データを読み出すとともに、前記特徴データ取得部が取得したユーザーの眼の映像の特徴データとを照合して、ユーザーがカード所有者本人かどうかの確認を行う照合部を備え、

サーバ側には、正規のユーザーの識別コードを格納した識別コードファイルを備え、

クライアント側で前記照合処理の結果、ユーザーがカード所有者本人と確認したとき、クライアントからサーバに識別コードが送信され、

サーバは、識別コードファイルを参照して、ユーザーへのサービスを開始することを特徴とするネットワークセキュリティシステム。

【請求項３】　クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、

クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録されたファイル検索キーと、ユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取ったファイル検索キーにより、クライアントに対してネットワークを介して接続された登録特徴データファイルから、カード所有者の登録特徴データを読み出して、前記特徴データ取得部が取得したユーザーの眼の映像の特徴データと照合し、ユーザーがカード所有者本人かどうかの確認を行う照合部を備え、

サーバ側には、正規のユーザーの識別コードを格納した識別コードファイルを備え、

クライアント側で前記照合処理の結果、ユーザーがカード所有者本人と確認したとき、クライアントからサーバに識別コードが送信され、

サーバは、識別コードファイルを参照して、ユーザーへのサービスを開始することを特徴とするネットワークセキュリティシステム。

【請求項４】　請求項１から３のいずれか１項において、

サーバは、クライアントに対して、照合処理の開始を要求してからその結果の通知を受けるまでの時間を監視して、その時間が妥当な時間範囲外である場合に、不正処理と判断することを特徴とするネットワークセキュリティシステム。

【請求項５】　クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、

クライアント側には、ユーザーの眼の映像を取得するカメラを備え、

サーバ側には、ネットワークを通じてクライアントから受信した眼の映像のビットマップデータから特徴データを取得し、この特徴データと、予め正規のユーザーから取得した登録特徴データファイルを参照して得た登録特徴データとを照合し、ユーザーがカード所有者本人かどうかの確認を行う照合部を備えたことを特徴とするネットワークセキュリティシステム。

【請求項６】　請求項５において、クライアント側から入力された識別コードをネットワーク介してサーバが受信し、この識別コードを用いて登録特徴データファイルから該当する登録特徴データもしくは登録特徴データ群を読み出して、照合部による照合対象とすることを特徴とするネットワークセキュリティシステム。

【請求項７】　クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、

クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録された登録特徴データとユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取った登録特徴データを用いてユーザーがカード所有者本人かどうかの確認を行う照合部とを備え、

サーバ側には、正規のユーザーの識別コードと登録特徴データもしくは登録特徴データ群とを対応させて格納した登録特徴データファイルを備え、

クライアントで読み込んだ識別コードがサーバに送信されると、サーバでは、登録特徴データファイルを参照し

て、対応する登録特徴データもしくは登録特徴データ群を得てクライアントに送信し、
クライアントの照合部は、サーバから受信した登録特徴データもしくは登録特徴データ群と、前記カード入力部が読み取った登録特徴データと、特徴データ取得部が取得したユーザーの眼の映像の特徴データとを相互に照合して、ユーザーがカード所有者本人かどうかの確認を行い、
前記照合処理の結果、ユーザーがカード所有者本人と確認したとき、その旨がクライアントからサーバに通知され、
サーバでは、その通知に基づいてサービスを開始することを特徴とするネットワークセキュリティシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークを通じて決裁等を行う場合の安全を確保するネットワークセキュリティシステムに関する。
【０００２】
【従来の技術】マルチメディアパソコンと呼ばれるパーソナルコンピュータは、音声や画像等を扱うことができ、電子メールその他各種の情報送受信に広く利用されている。また、インターネットに代表されるような巨大なネットワークには、このような端末を接続し、商取引を含む様々なサービスが提供されている。このようなネットワークを通じた取引を行う場合、取引を成立させるために所定の決裁が必要となる。しかしながら、ネットワーク上をパスワードやキャッシュカードのコードデータ等を伝送した場合に、いわゆるハッカー等によりそのデータが盗まれて悪用されるおそれがある。従って、一般には決裁は申込用紙の郵送や銀行の窓口における振込処理等で実行されている。
【０００３】
【発明が解決しようとする課題】しかしながら、従来のような決裁の方法は、ユーザーにとって煩わしいことからネットワークを用いた取引の利便性に欠ける。こうした点を解決するため、暗号化技術が広く研究されている。これでも必ずしもハッカーに対し完全な防御がなされるとは限らない。
【０００４】一方、例えば入場者管理等のために、眼の映像から取得される特徴データを利用して、本人を確認する技術が開発されている（特公平５－８４１６６号公報）。ここでは、眼の映像の一部であるアイリスデータを処理した所定の特徴データを得て、指紋等と同様にして本人であるかどうかの判断をしている。この種の技術をネットワークにおける取引の安全確保に利用することが好ましい。
【０００５】
【課題を解決するための手段】本発明は以上の点を解決するため次の構成を採用する。

〈構成１〉クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録された登録特徴データと、ユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取った登録特徴データと特徴データ取得部が取得したユーザーの眼の映像の特徴データとを照合して、ユーザーがカード所有者本人かどうかの確認を行う照合部を備え、サーバ側には、正規のユーザーの識別コードを格納した識別コードファイルを備え、クライアント側で上記照合処理の結果、ユーザーがカード所有者本人と確認したとき、クライアントからサーバに識別コードが送信され、サーバは、識別コードファイルを参照して、ユーザーへのサービスを開始することを特徴とするネットワークセキュリティシステム。
【０００６】〈構成２〉クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録されたファイル検索キーと、ユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取ったファイル検索キーにより登録特徴データファイルからカード所有者の登録特徴データを読み出すとともに、上記特徴データ取得部が取得したユーザーの眼の映像の特徴データとを照合して、ユーザーがカード所有者本人かどうかの確認を行う照合部を備え、サーバ側には、正規のユーザーの識別コードを格納した識別コードファイルを備え、クライアント側で上記照合処理の結果、ユーザーがカード所有者本人と確認したとき、クライアントからサーバに識別コードが送信され、サーバは、識別コードファイルを参照して、ユーザーへのサービスを開始することを特徴とするネットワークセキュリティシステム。
【０００７】〈構成３〉クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録されたファイル検索キーと、ユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取ったファイル検索キーにより、クライアントに対してネットワークを介して接続された登録特徴データファイルから、カード所有者の登録特徴データを読み出して、上記特徴データ取得部が取得したユーザーの眼の映像の特徴データと照合し、ユーザーがカード所有者本人かどうかの確認を行う照合部を備え、サーバ側には、正規のユーザーの識別コードを格納した識別コー

ドファイルを備え、クライアント側で上記照合処理の結果、ユーザーがカード所有者本人と確認したとき、クライアントからサーバに識別コードが送信され、サーバは、識別コードファイルを参照して、ユーザーへのサービスを開始することを特徴とするネットワークセキュリティシステム。

【０００８】〈構成４〉構成１から３のいずれか１項において、サーバは、クライアントに対して、照合処理の開始を要求してからその結果の通知を受けるまでの時間を監視して、その時間が妥当な時間範囲外である場合に、不正処理と判断することを特徴とするネットワークセキュリティシステム。

【０００９】〈構成５〉クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像を取得するカメラを備え、サーバ側には、ネットワークを通じてクライアントから受信した眼の映像のビットマップデータから特徴データを取得し、この特徴データと、予め正規のユーザーから取得した登録特徴データファイルを参照して得た登録特徴データとを照合し、ユーザーがカード所有者本人かどうかの確認を行う照合部を備えたことを特徴とするネットワークセキュリティシステム。

【００１０】〈構成６〉構成５において、クライアント側から入力された識別コードをネットワーク介してサーバが受信し、この識別コードを用いて登録特徴データファイルから該当する登録特徴データもしくは登録特徴データ群を読み出して、照合部による照合対象とすることを特徴とするネットワークセキュリティシステム。

【００１１】〈構成７〉クライアントとサーバがネットワークを介して相互に接続され、クライアントの要求に従ってサーバが所定のサービスを提供するものにおいて、クライアント側には、ユーザーの眼の映像から特徴データを取得する特徴データ取得部と、ユーザーが投入したカードに記録された登録特徴データとユーザーの識別コードとを読み込むカード入力部と、このカード入力部が読み取った登録特徴データを用いてユーザーがカード所有者本人かどうかの確認を行う照合部とを備え、サーバ側には、正規のユーザーの識別コードと登録特徴データもしくは登録特徴データ群とを対応させて格納した登録特徴データファイルを備え、クライアントで読み込んだ識別コードがサーバに送信されると、サーバでは、登録特徴データファイルを参照して、対応する登録特徴データもしくは登録特徴データ群を得てクライアントに送信し、クライアントの照合部は、サーバから受信した登録特徴データもしくは登録特徴データ群と、上記カード入力部が読み取った登録特徴データと、特徴データ取得部が取得したユーザーの眼の映像の特徴データとを相互に照合して、ユーザーがカード所有者本人かどうかの確認を行い、上記照合処理の結果、ユーザーがカード所有者本人と確認したとき、その旨がクライアントからサーバに通知され、サーバでは、その通知に基づいてサービスを開始することを特徴とするネットワークセキュリティシステム。

【００１２】

【発明の実施の形態】以下、本発明の実施の形態を具体例を用いて説明する。

〈具体例１〉図１は、具体例１のシステムを示すブロック図である。このシステムのクライアント１がネットワーク２を介してサーバ３に接続され、クライアント１を操作するユーザーがサーバ３の各種のサービスを受ける構成となっている。クライアント１もサーバ３も例えばパーソナルコンピュータやワークステーションにより構成される。クライアント１には、特徴データ取得部４、カード入力部６、照合部７が接続されている。特徴データ取得部４は、ユーザー９の眼の映像を図示しないカメラ等で撮影し、既に説明したようなアイリスデータあるいはその他の眼の各部の特徴をデータ化した特徴データを取得する部分である。カード入力部６は、磁気カードやＩＣカードのようなカード５を装着することによって、その中に記憶されたデータを読み込むための装置である。

【００１３】カード５には、ユーザー９が予め登録した登録特徴データ１２と、ユーザー９の取引に使用される識別コード１３が格納されている。照合部７は、特徴データ取得部４から入力する取得特徴データ１１と、カード入力部６から入力する登録特徴データ１２とを比較照合して、ユーザー９が本人のカード５を使用しているかどうかを判断する部分である。本人と判断された場合に、照合部７は、カード入力部６から受け入れた識別コード１３をクライアント１に出力する構成となっている。識別コード１３はネットワーク２を通じてサーバ３に送られる。

【００１４】サーバ３はクライアント１から送られた識別コードを受信して、識別コードファイル８を参照し、所定のサービス提供のためのアクセス処理等を許可する装置である。このサーバ３にアクセスを許可された場合、ユーザー９は所定の取引処理を実行しあるいは各種のサービスを受けて所定の決裁を実行することができる。なお、サーバ３は、識別コードを受け入れた場合に識別コードファイル８に格納されたデータを読み出し、ユーザー９に関する情報を取得し、その情報に基づいて各種のサービスを行う。また、必要に応じてクライアント１側にユーザーの情報を送り、ユーザー９による確認処理等を行うこともできる。

【００１５】図２には、具体例１のシステム動作フローチャートを示す。この図によって、図１に示した具体例１のシステムの動作を説明する。まず、ステップＳ１において、クライアント１からサーバ３に対しアクセス要求が行われると、サーバ３はこれに対して特徴データの

照合要求を行う。

【００１６】次に、ステップＳ２において、クライアント１が特徴データ取得部４を動作させてユーザー９の眼の映像を取得する。そして、所定の処理により特徴データを取得する。更に、ステップＳ３において、カード５から登録特徴データ１２を読み取る。次に、ステップＳ４において、照合部７は、照合処理を行う。ステップＳ５において、カードの所持者が本人であると確認されるとステップＳ６に進み、カードから読み取った識別コードをサーバ３へ送信する。サーバ３はこれを受信し、ステップＳ７において、識別コードファイル８を参照し、所定のユーザーに対する情報や属性データ等を得る。こうして、サーバ３はクライアント１にアクセスを許可しサービスを開始する。

【００１７】なお、ステップＳ５において、本人でないと確認された場合はステップＳ８に進み、処理を中止する。ここで、クライアント１に対し、再度眼の映像の入力あるいはカードの投入を要求するようにしてもよい。

【００１８】〈具体例１の効果〉この例によれば、クライアント側でアイリスデータのような眼の映像の特徴データを使用して本人確認を行うため、第三者の利用を阻止し、セキュリティが高められる。しかも、ネットワークに流れるデータはサーバ３からの要求とその応答である識別コード１３のみのため、特徴データや暗証番号のような個人情報をネットワークに流すことはない。このため、個人情報漏洩による悪用を防止できる。しかも、ユーザー本人は知ることのできないような識別コードを利用することによって、識別コードが他人に盗まれる危険も減少し、商取引のセキュリティを向上させる。

【００１９】〈具体例２〉図３に、具体例２のシステムブロック図を示す。このシステムも、クライアント１がネットワーク２を介してサーバ３に対し所定のアクセス要求を行う構成となっている。クライアント１に接続された特徴データ取得部４、カード入力部６、照合部７等の構成は具体例１と同様である。この具体例２では、新たに登録特徴データファイル１５が照合部７に接続される。登録特徴データファイル１５には、所定のファイル検索キー１４と登録特徴データ１２とが対応付けらて格納されている。

【００２０】また、カード５には、このファイル検索キー１４と識別コード１３とが格納される。照合部７は、ファイル検索キー１４を使用して登録特徴データファイル１５を検索し、対応する登録特徴データ１２を読み出す。そして、その登録特徴データ１２と特徴データ取得部４から入力する取得特徴データ１１との照合処理を行うように構成されている。その他の構成は具体例１と同様である。

【００２１】図４を用いて、具体例２の動作を説明する。図４は、具体例２のシステム動作フローチャートである。図のステップＳ１では、具体例１と同様、クライアントからのアクセス要求に対しサーバが特徴データの照合要求を行い、ステップＳ２ではクライアントがユーザーの眼の映像を取得する。次に、ステップＳ３では、ユーザー９が投入したカード５からファイル検索キー１４を読み込む。ステップＳ４で、照合部７は登録特徴データファイル１５を参照して、ファイル検索キー１４に対応する登録特徴データ１２を読み出す。そして、ステップＳ５において、特徴データ取得部４から入力した取得特徴データ１１との照合処理を行う。この照合の結果、本人と判断されると、ステップＳ６からステップＳ７に進み、識別コード１３をサーバ３へ送信する。以下の処理は具体例１と同様で、ステップＳ８ではサーバが識別コードを用いたサービスを開始する。本人と判断されなければ処理が中止される（ステップＳ９）。

【００２２】〈具体例２の効果〉具体例１と比較すると、カード５に登録特徴データを格納せず、ファイル検索キーを格納するようにしたので、カード５に格納すべきデータ量を十分に少なくできる。従って、簡単な磁気カード等でカードを実現することができ、取引コストを削減できる。その他の効果は具体例１と同様である。

【００２３】〈具体例３〉図５に、具体例３のシステムブロック図を示す。この図に示すように、具体例３では、登録特徴データファイル１５をクライアント１に対し第１ネットワーク２Ａを介して接続している。この第１ネットワーク２Ａは、例えばＬＡＮ（ローカルエリアネットワーク）のような、ネットワーク上のデータの秘密を確保しやすいネットワークとする。この第１ネットワーク２Ａには、図示しない他のクライアントが多数接続されているものとする。また、登録特徴データファイル１５には、ファイル検索キー１４と登録特徴データ群１８とが格納されている。

【００２４】図３に示した具体例２のシステムとこの具体例３のシステムとを比較すると、登録特徴データファイル１５がクライアント１に対し第１ネットワーク２Ａを介して接続されている点のみが異なる。なお、登録特徴データファイル１５に格納されたファイル検索キー１４に対応する登録特徴データ群１８は、登録特徴データ全体を適当に分割した登録特徴データの集合である。

【００２５】照合部７は照合処理を行う場合、クライアントと第１ネットワーク２Ａを通じて登録特徴データファイル１５を検索し、必要な登録特徴データ群１８を取得する。その後、照合処理を実行する。その他の動作は図３に示すものと全く同一である。図３に示した具体例２に示すように、ファイル検索キーと登録特徴データとを一対一で対応させてもよい。また逆に、具体例２の場合にも、ファイル検索キー１４に対応させて登録特徴データ群を格納してもよい。この場合、照合部７は登録特徴データ群の中に取得特徴データ１１と一致するものがあるかどうかを判断することになる。具体例３においても同様で、照合部７は第１ネットワーク２Ａを通じて受

け入れた登録特徴データ群１８と取得特徴データ１１との照合処理を行う。１個のファイル検索キーで複数の登録特徴データを取り出すのは、全ての登録特徴データに対応するファイル検索キーを用意するとファイル検索キーの文字数が著しく増加して管理が容易でなくなるからである。また、照合処理が比較的速やかにできる程度に登録特徴データを取り出せば、後は照合部７によって照合処理を行えばよいからである。

【００２６】〈具体例３の効果〉具体例２の効果に加えて、登録特徴データファイル１５が第１ネットワーク２Ａに接続されているため、この第１ネットワーク２Ａに接続された他のクライアントも自由にこの登録特徴データファイル１５を参照できる。従って、クライアント側に大きな登録特徴データファイルを保存しておく必要がなくなる。もちろん、登録特徴データファイル１５は１つでなく、任意の数だけ第１ネットワーク２Ａに接続されても構わない。これによって、クライアント側に特徴データの照合部さえあれば自由にネットワークと接続しシステムの拡張が可能になる。また、登録特徴データファイル１５の増減変更が容易にできるためメンテナンス性が向上し、維持コストが削減できる。

【００２７】〈具体例４〉図６には、具体例４のシーケンスチャートを示す。この具体例４では、サーバがクライアントからアクセス要求を受けた場合に、クライアントが実際に特徴データの照合処理を実行しているかどうかを監視し、その処理時間等から不正な処理を排除する。この具体例４を適用するシステムは、図１、図３、図５等により説明されたどのシステムであってもよい。

【００２８】図６において、まずステップＳ１で、クライアント１がサーバ３に対しアクセスを要求する。サーバ３はこれに対応してステップＳ２でクライアント１に対し特徴データの照合要求を行う。クライアント１はステップＳ３において、その照合準備を行う。即ち、例えば図１のシステムでは、ユーザー９の眼の映像を特徴データ取得部４が取得し、特徴データの生成処理を行う。次に、ステップＳ５において、サーバ３に対し準備完了報告を行う。一方、サーバ３はステップＳ２でクライアント１に対し特徴データの照合要求を行った後、タイマによる監視を行う（ステップＳ４）。

【００２９】即ち、照合要求から準備完了報告までの時間を監視し、クライアント１の側で適切な処理を行った後に準備完了報告Ｓ５が受け入れられたかどうかを判断する。著しく報告までの時間が長い場合や異常に短い場合には何らかの不正が生じたとして取引を停止する。不正を検出した場合にはステップＳ１０に進み、取引停止処理等を行う。更に、ステップＳ５で準備完了報告を受けたサーバ３は、ステップＳ６で照合スタート指示を行う。これに対しクライアント１は、ステップＳ７において照合処理を実行し、ステップＳ９において結果通知を報告する。サーバ３は、この場合にも照合スタート指示Ｓ６をクライアント１に送った時点から結果通知をステップＳ９で受信するまでタイマ監視を行う（ステップＳ８）。

【００３０】ここでも、必要な照合処理のための時間を考慮し、著しく短い場合と著しく長い場合とを不正処理と判定する。このようにして、実際の特徴データ照合処理を行っているか、この処理を行わずに例えば識別コードを直ちに送信してきているか等を区別することができる。

【００３１】〈具体例４の効果〉以上のように、クライアントによる照合準備等を含む照合処理時間をサーバが監視するので、不正処理を排除してセキュリティを高められる。例えば、予め不正に取得した特徴データを用いてすぐに準備完了報告がきたり、照合処理ができるはずのないような短時間に識別コードが返ってくると、不正に準備されたものと判断できる。

【００３２】〈具体例５〉図７には、具体例５のシステムブロック図を示す。このシステムもクライアント１がネットワーク２を介してサーバ３に接続されている。また、このシステムでは、クライアント１に対してカメラ１６が接続され、ユーザー９の眼の映像を取得する構成となっている。また、サーバ３の側には登録特徴データファイル１５及び照合部７が設けられる。

【００３３】上記の構成のシステムは、次のように動作する。図８には、具体例５の動作フローチャートを示す。図のステップＳ１において、まずクライアント１からのアクセス要求がサーバ３に到着すると、サーバ３はクライアント１のカメラ１６に対し起動要求を行う。ステップＳ２では、クライアント１がカメラ１６を用いてユーザー９の眼の映像を取得し、眼の映像のビットマップデータ１７をネットワーク２を通じてサーバ３に送信する。

【００３４】ここで、サーバ３では、具体例１や具体例２で実行したクライアント側による眼の映像の特徴データ取得処理をサーバ側で行う（ステップＳ３）。次に、ステップＳ４において、サーバ側で登録特徴データファイル１５を参照して照合処理を実行する。即ち、サーバ側には眼の映像のビットマップデータが転送され、ここからサーバ側において特徴データを取得し、登録特徴データファイルとの照合が行われる。ステップＳ５で本人と確認されると、ステップＳ６で所定のサービスその他の処理が開始される。一方、本人と確認されないとステップＳ５からステップＳ７に進み、処理が中止される。

【００３５】〈具体例５の効果〉ビデオカメラのような撮影機材によってユーザーの眼の映像が直接サーバ側に送られ、サーバ側で特徴データの照合処理等を実行するため、登録特徴データの集中管理が行えるという効果がある。しかも、眼の映像そのものを送信するため、識別データや暗証番号、その他のように簡単に解読できる内容でないためセキュリティの向上が期待できる。また、

一般のマルチメディアパソコンに設けられた簡単なビデオカメラを用いてサーバに対しアクセス要求を実行することができるため、クライアント側の設備費用が安価にできるという効果がある。

【００３６】〈具体例６〉図９には、具体例６のシステムブロック図を示す。このシステムは、具体例５の場合と比較すると、クライアント１の側にキーボード２１のような入力手段を設け、識別コード１３を入力できるようにしている点が異なる。その他の部分は具体例５と同様である。

【００３７】図１０に、具体例６のシステム動作フローチャートを示す。ここでも、具体例５の場合と同様に、ステップＳ１でクライアントからのアクセス要求に対しカメラが起動し、ステップＳ２でカメラが撮影した眼の映像をサーバ３へ送信する。サーバ側では、その眼の映像について特徴データを取得する。更に、この具体例６では、ステップＳ４において、クライアント側で識別コード１３をキーボード２１を用いて入力する。

【００３８】この識別コードはネットワーク２を通じてサーバ３に送られる。サーバ３の照合部７は、登録特徴データファイル１５を参照し、識別コード１３に対応する登録特徴データ群１８を取り出す。その後、この登録特徴データ群１８とサーバ３で生成した取得特徴データとの照合処理が行われる。識別コード１３と登録特徴データとは、１対１で格納されていてもよいし、登録特徴データ群が１つの識別コード１３と対応するように格納されていてもよい。いずれの場合にも、大量の登録特徴データの中から一部の登録特徴データが取り出されて照合処理を行うため、処理時間を短縮できる効果がある。

【００３９】〈具体例６の効果〉クライアント側からキーボードを用いて識別コードを入力し、サーバ側での照合対象となる登録特徴データを絞り込むことができるため、照合処理のスピードアップが図られる。また、演算量も少なくなるため、サーバのマシンをローパワーの安価なマシンに置き換えることができるという効果がある。

【００４０】〈具体例７〉図１１に、具体例７のシステムブロック図を示す。このシステムの構成は、クライアント側とネットワークについては図１に示したシステムと同様である。サーバ３の側には登録特徴データファイル１５が設けられ、ここには識別コード１３と登録特徴データ１２とを対応付けたデータが格納されている。

【００４１】図１２には、具体例７のシステム動作フローチャートを示す。このシステムは次のように動作する。まず、ステップＳ１において、クライアントからのアクセス要求に対してサーバが特徴データの照合要求を行う。ステップＳ２では、クライアントがユーザーの眼の映像を取得し、ステップＳ３において、カードから登録特徴データを読み取る。ステップＳ４では、クライアント側でカードから識別コードを読み取る。そして、ステップＳ５で、その識別コードをサーバ側に送り、サーバ側で登録特徴データファイル１５から識別コードに対応するデータを読み出す。ステップＳ６では、読み出した登録特徴データをクライアント側に送る。

【００４２】即ち、この具体例では、クライアント側にカードから読み出した登録特徴データとサーバで読み出した登録特徴データとが送り込まれ、クライアント側で取得した眼の映像から得た特徴データと３つが同時に照合処理される。ステップＳ７において、この照合処理を行うと、ステップＳ８で本人かどうかの判断がなされ、本人と判断されるとステップＳ９で処理が続行され、本人でないと判断されるとステップＳ１０に進み、処理が中止される。

【００４３】〈具体例７の効果〉３種類の特徴データが相互に照合処理されることから、これまでのシステムよりも更に本人確認のためのセキュリティが高まる。

【図面の簡単な説明】

【図１】具体例１のシステムブロック図である。

【図２】具体例１のシステム動作フローチャートである。

【図３】具体例２のシステムブロック図である。

【図４】具体例２のシステム動作フローチャートである。

【図５】具体例３のシステムブロック図である。

【図６】具体例４のシーケンスチャートである。

【図７】具体例５のシステムブロック図である。

【図８】具体例５のシステム動作フローチャートである。

【図９】具体例６のシステムブロック図である。

【図１０】具体例６のシステム動作フローチャートである。

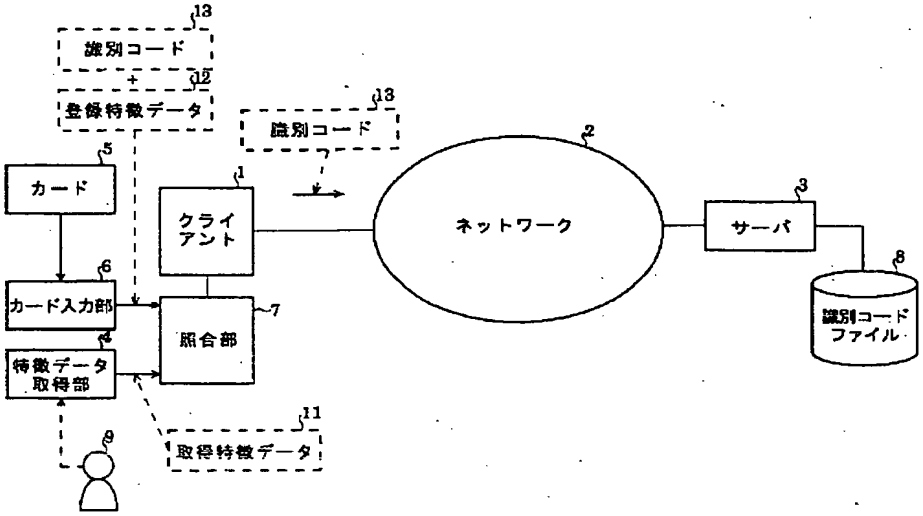
【図１１】具体例７のシステムブロック図である。

【図１２】具体例７のシステム動作フローチャートである。

【符号の説明】

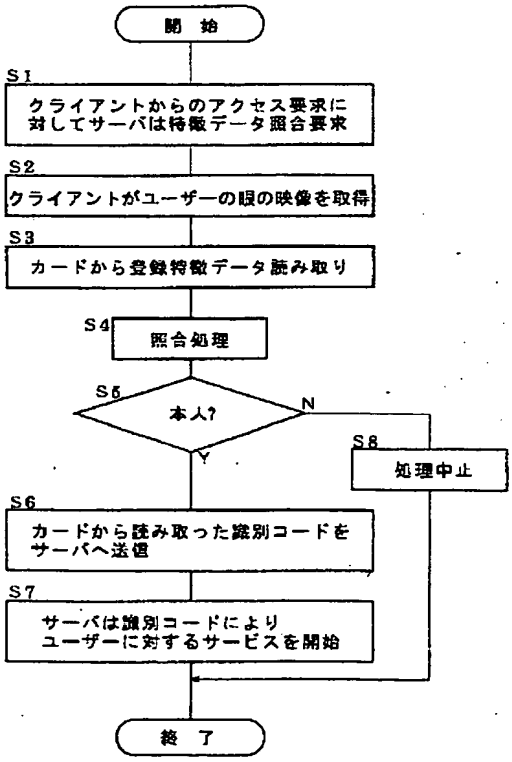
１　クライアント
２　ネットワーク
３　サーバ
４　特徴データ取得部
５　カード
６　カード入力部
７　照合部
８　識別コードファイル

【図１】



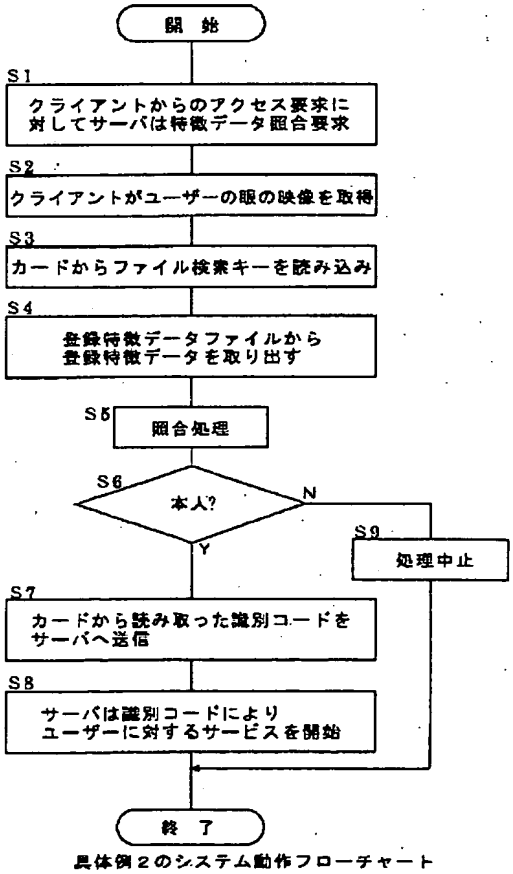
具体例１のシステムブロック図

【図２】



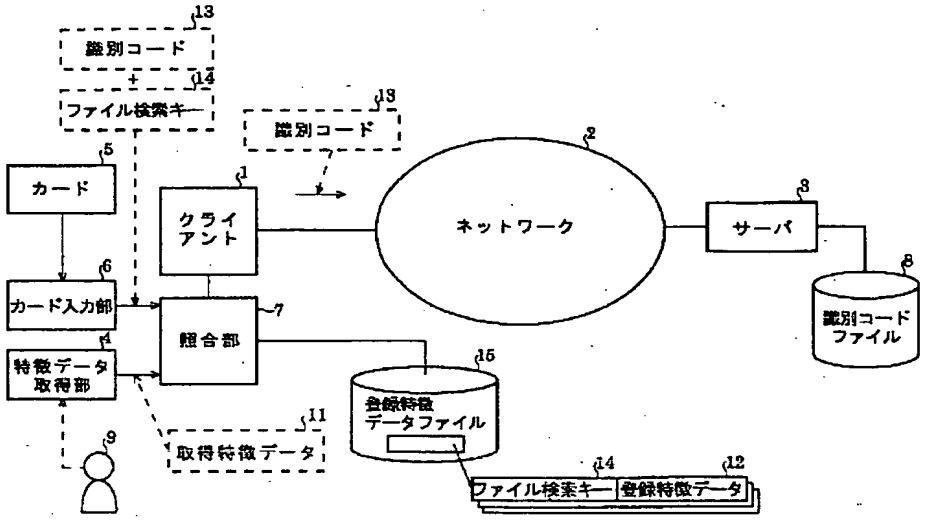
具体例１のシステム動作フローチャート

【図４】



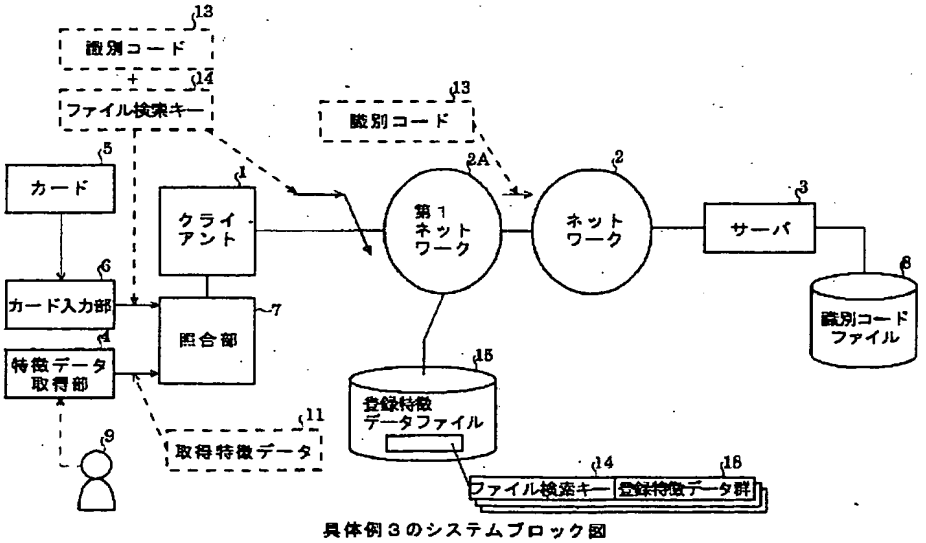
具体例２のシステム動作フローチャート

【図３】



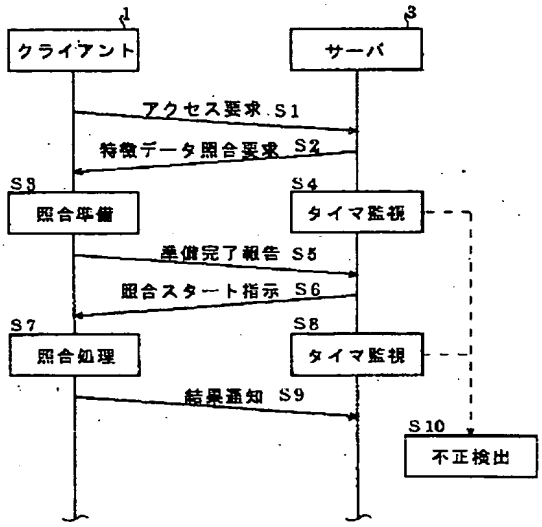
具体例２のシステムブロック図

【図５】



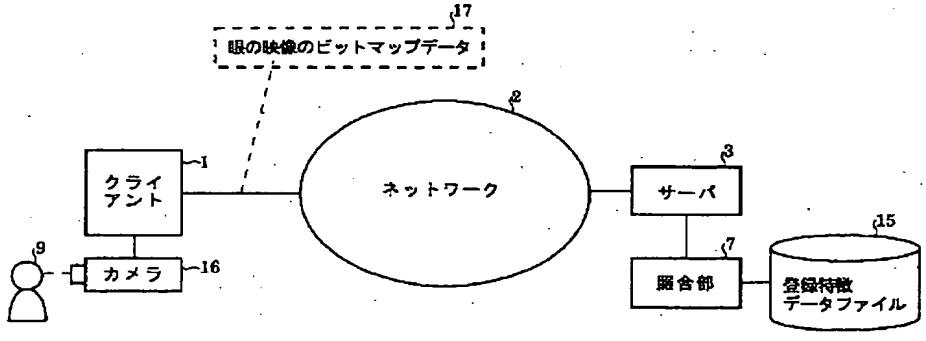
具体例３のシステムブロック図

【図６】



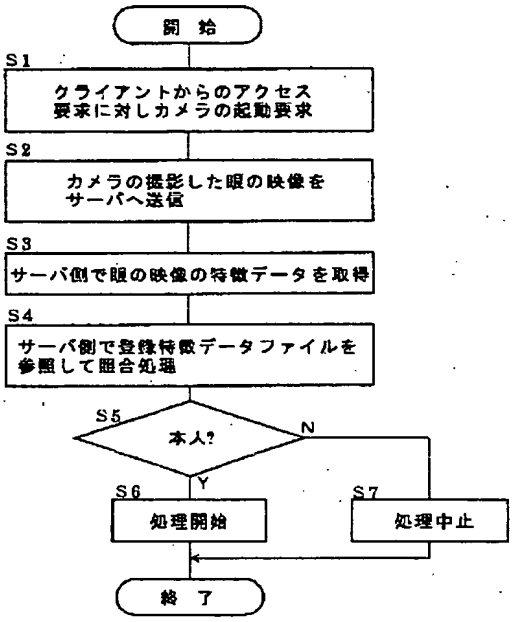
具体例４のシーケンスチャート

【図７】



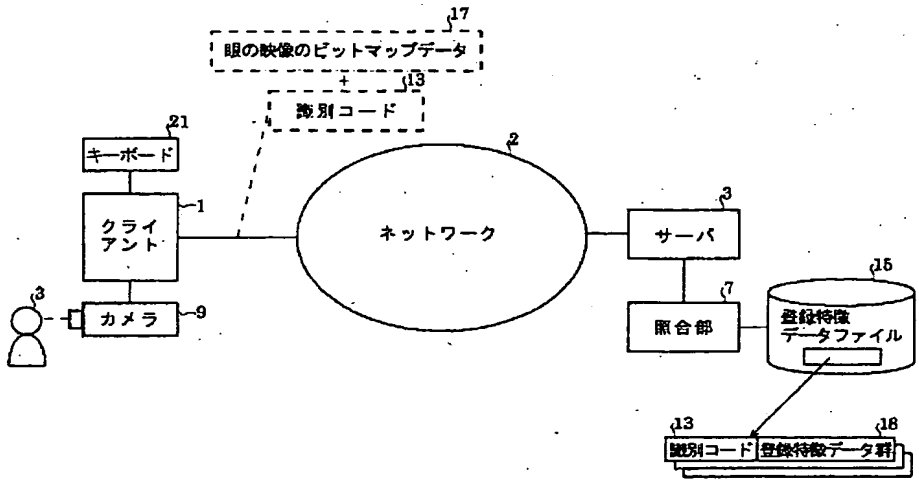
具体例５のシステムブロック図

【図８】



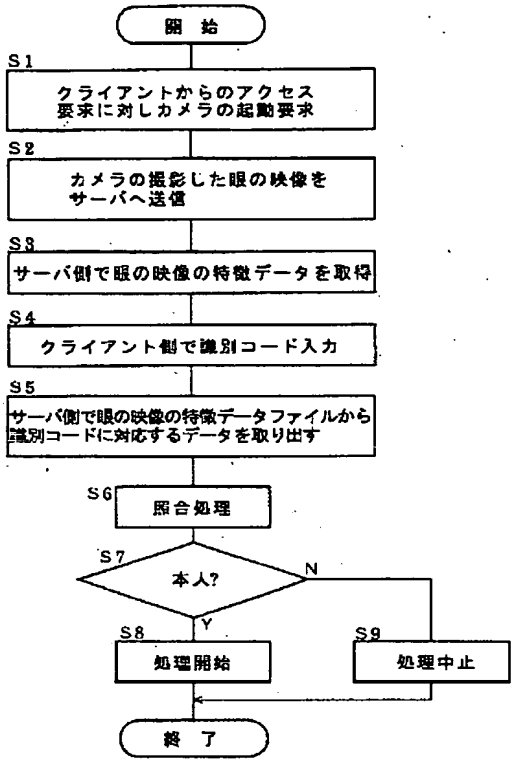
具体例５のシステム動作フローチャート

【図９】



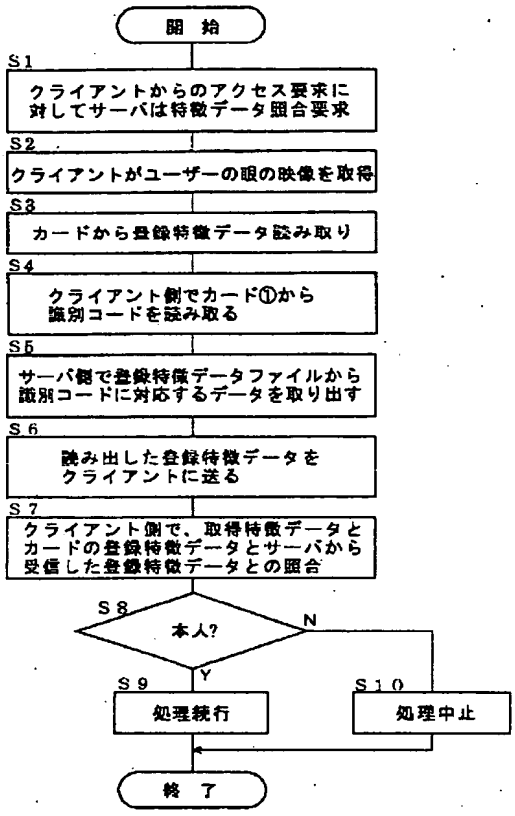
具体例６のシステムブロック図

【図１０】



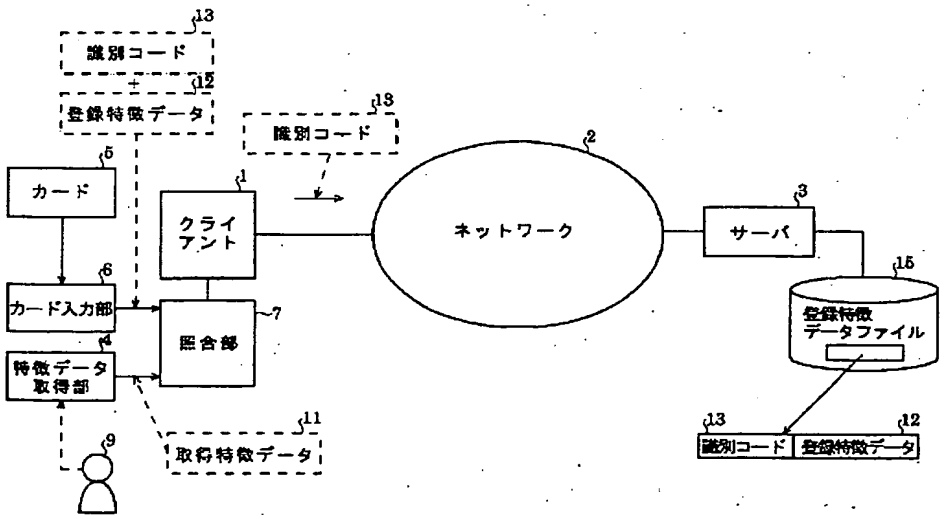
具体例６のシステム動作フローチャート

【図１２】



具体例７のシステム動作フローチャート

【図１１】



具体例７のシステムブロック図

フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
Ｇ０６Ｔ 7/00		Ｇ０６Ｆ 15/62	４６５Ａ